国家互联网应急中心

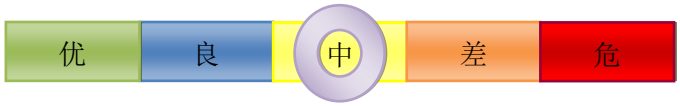
网络安全信息与动态周报

2016 年第 20 期

5 月 9 日-5 月 15 日

CNCERT/CC

本周网络安全基本态势

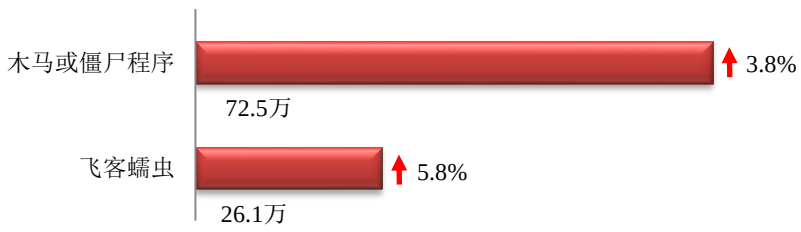


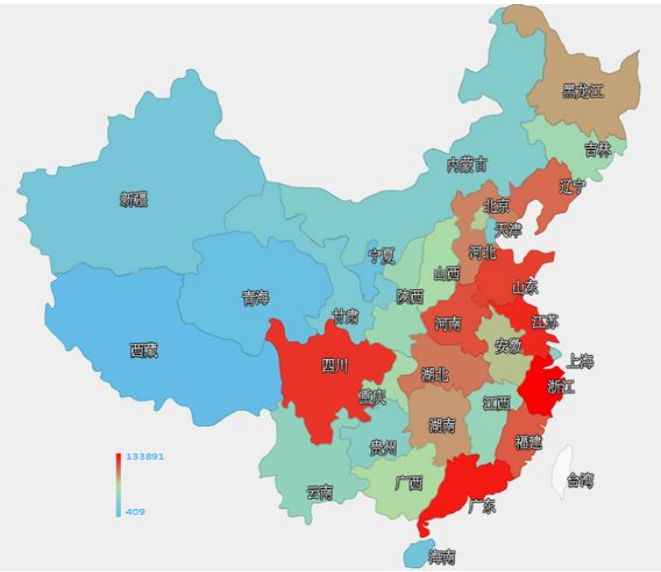
境内感染网络病毒的主机数量	•98.6万	4.3%
境内被篡改网站总数 其中政府网站数量	•3342 •85	0.9% 5.6%
境内被植入后门网站总数 其中政府网站数量	•14063 •415	26.4% 27.7%
针对境内网站的仿冒页面数量	•2763	39.8%
新增信息安全漏洞数量 其中高危漏洞数量	•278 •112	110.6% 300.0%

表示数量与上周相同 *表示数量较上周环比增加* *表示数量较上周环比减少*

本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 98.6 万个，其中包括境内被木马或被僵尸程序控制的主机约 72.5 万以及境内感染飞客（conficker）蠕虫的主机约 26.1 万。



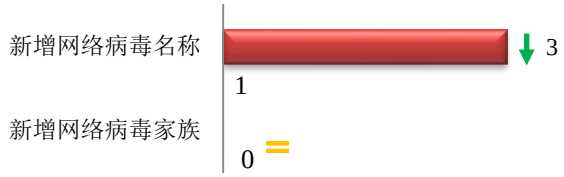


木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是浙江省、广东省和江苏省。

TOP3

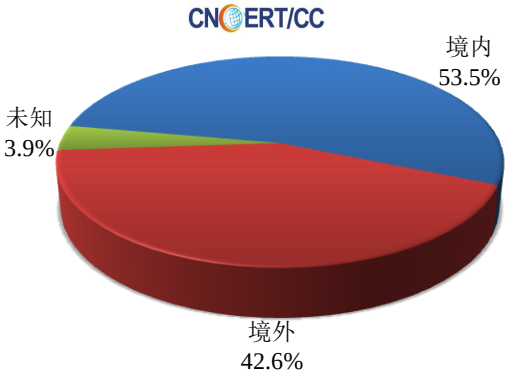
浙江省	•约13.4万个（约占中国大陆总感染量的18.0%）
广东省	•约10.0万个（约占中国大陆总感染量的13.4%）
江苏省	•约6.6万个（约占中国大陆总感染量的8.9%）

本周 CNCERT 捕获的新增网络病毒文件，按网络病毒名称统计新增 1 个，按网络病毒家族统计无新增。

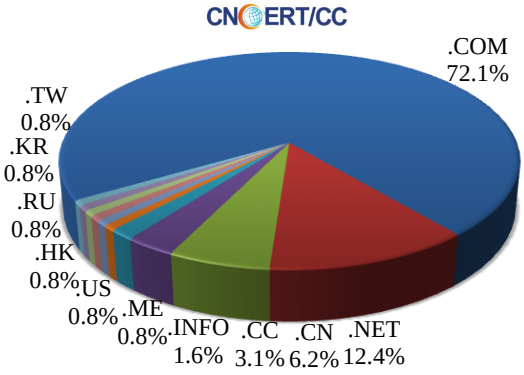


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 129 个，涉及 IP 地址 335 个。在 129 个域名中，有 42.6%为境外注册，且顶级域为.com 的约占 72.1%；在 335 个 IP 中，有约 10.7%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 32 个 IP。

本周放马站点域名注册所属境内外分布
(5/9-5/15)



本周放马站点域名所属顶级域的分布
(5/9-5/15)



针对 CNCERT 自主监测发现以及各单位报送数据，CNCERT 积极协调域名注册机构等进行处理，同时通过 ANVA 在其官方网站上发布恶意地址黑名单。

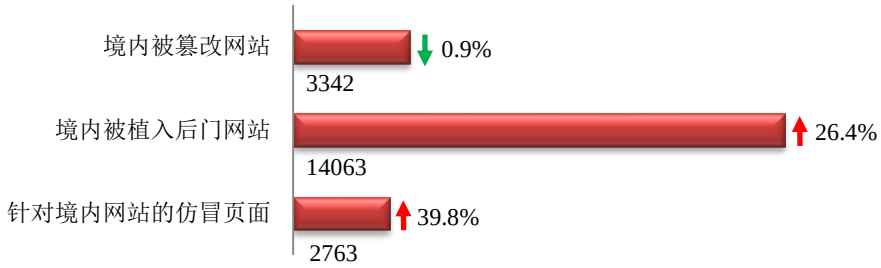
ANVA恶意地址黑名单发布地址

http://www.anva.org.cn/virusAddress/listBlack

中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写 ANVA）是由中国互联网协会网络与信息安全工作委员会发起、CNCERT 具体组织运作的行业联盟。

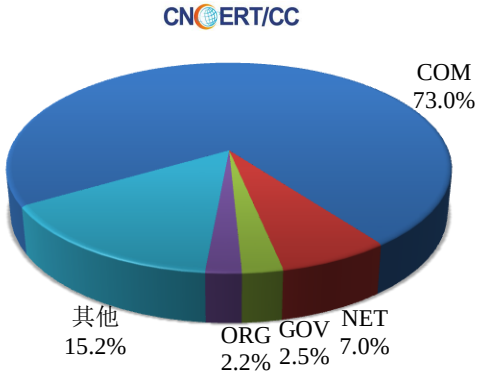
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 3342 个；境内被植入后门的网站数量为 14063 个；针对境内网站的仿冒页面数量为 2763。

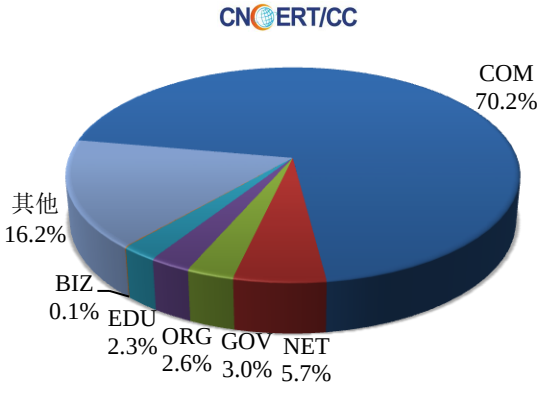


本周境内被篡改政府网站（GOV 类）数量为 85 个（约占境内 2.5%），较上周环比下降了 5.6%；境内被植入后门的政府网站（GOV 类）数量为 415 个（约占境内 3.0%），较上周环比上升了 27.7%；针对境内网站的仿冒页面涉及域名 1851 个，IP 地址 605 个，平均每个 IP 地址承载了约 5 个仿冒页面。

本周我国境内被篡改网站按类型分布
(5/9-5/15)

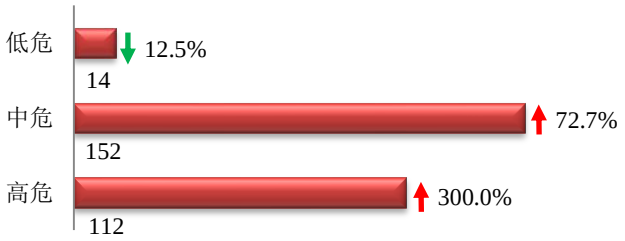


本周我国境内被植入后门网站按类型分布
(5/9-5/15)

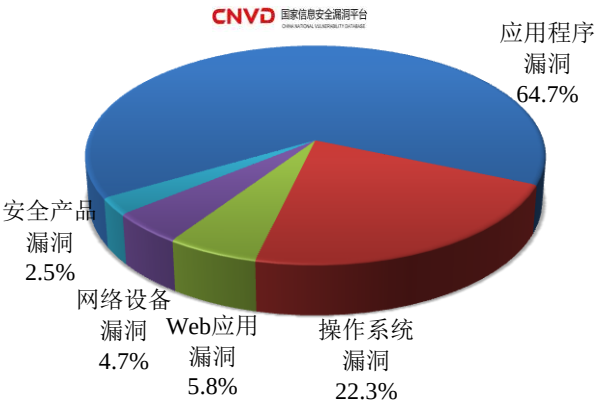


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 278 个，信息安全漏洞威胁整体评价级别为中。



本周CNVD收录漏洞按影响对象类型分布
(5/9-5/15)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是操作系统漏洞和 Web 应用漏洞。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

CNVD漏洞周报发布地址

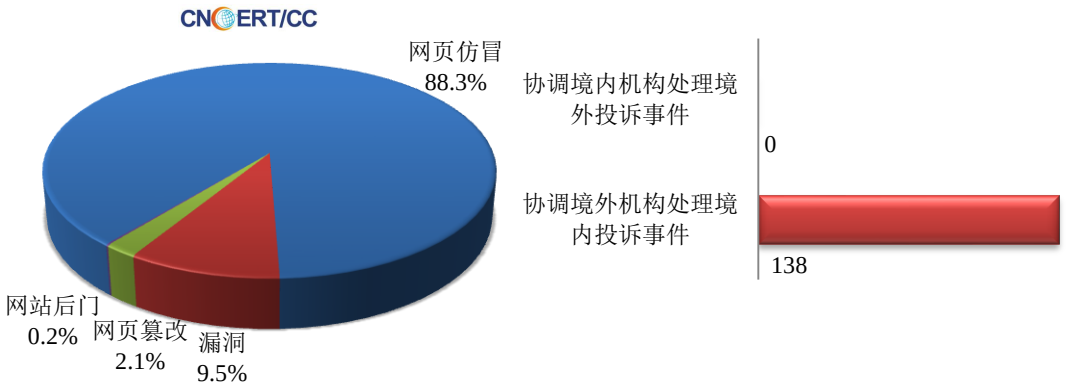
http://www.cnvd.org.cn/webinfo/list?type=4

国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

本周事件处理情况

本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 623 起，其中跨境网络安全事件 138 起。

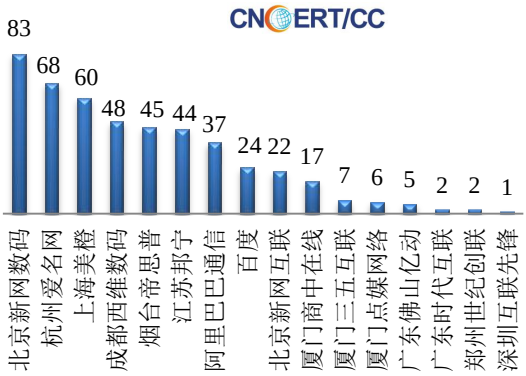
本周CNCERT处理的事件数量按类型分布
(5/9-5/15)



本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 550 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事 446 起和互联网服务提供商仿冒事件 94 起。

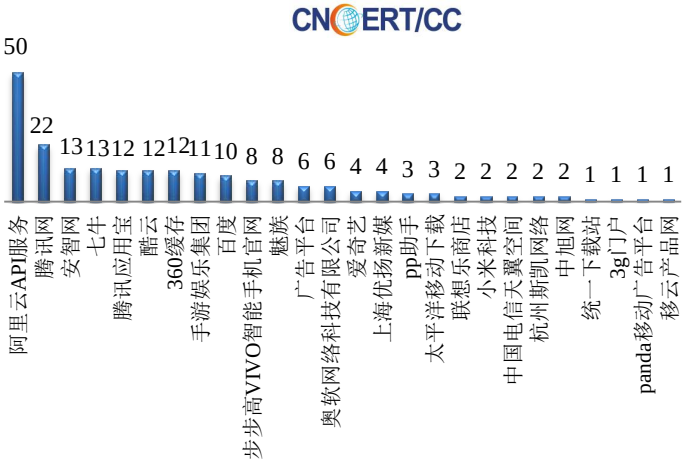
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(5/9-5/15)

本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (5/9-5/15)



本周，CNCERT 协调 26 个应用商店及挂载恶意程序的域名开展移动互联网恶意代码处理工作，共处理传播移动互联网恶意代码的恶意 URL 链接 211 个。

本周CNCERT协调手机应用商店处理移动互联网恶意代码事件数量排名 (5/9-5/15)



业界新闻速递

1、信安标委：加快制定网络安全信息共享指南

中国信息产业网 5 月 10 日消息 5 月 9 日，全国信息安全标准化技术委员会（以下简称“信安标委”）在北京召开座谈会，学习贯彻习近平总书记在网络安全和信息化工作座谈会上的重要讲话精神，与会同志表示，要抓紧制定国家关键信息基础设施认定指南、保护框架等重要标准，加快制定网络安全信息共享指南等标准。会议认为，习近平总书记的重要讲话，站在历史和全局的高度，深刻揭示了网络安全和信息化发展规律，对网络安全和信息化发展的重大问题作出了科学回答和战略部署。与会同志表示，要制定好标准、应用好标准，就要深刻领会和把握总书记重要讲话的精神实质，特别是要把总书记对网络安全规律的阐述，把总书记关于发展和安全、开放和自主、管理和服务重大关系的论断贯彻到网络安全标准化工作中。要深入贯彻总书记网络安全观，重点做好以下几个方面的工作。一是贯彻总书记关于以人民为中心和网络安全为人民、网络安全靠人民的指示，加快出台关于个人信息安全规范、保护指南等网络安全国家标准。二是贯彻总书记关于加快构建关键信息基础设施安全保障体系的指示，抓紧制定国家关键信息基础设施认定指南、保护框架等重要标准。三是贯彻总书记关于建立网络安全风险报告和信息共享机制的要求，加快制定网络安全信息共享指南等标准。四是贯彻总书记关于减少重复检测认证的要求，对现有检测认证标准进行全面梳理和修订，为统一规范网络安全产品检测认证工作提供标准保障。五是贯彻总书记关于下大功夫、下大本钱，建一流网络空间安全学院的指示，积极研究有关网络安全教材、学科专业建设、人才培养的评价指标。六是贯彻总书记关于积极参与国际网络空间标准和规则制定的指示，实质性参与国际网络安全标准化工作，大力推动国家标准上升为国际标准，更多地体现中国声音、中国主张。信安标委是国家标准委直属标委会，业务上受中央网信办指导，主要负责信息安全技术、机制、服务、管理、评估等领域的标准化技术工作。信安标委要在总书记重要讲话精神的指引下，认真履责、不辱使命，围绕中心、服务大局，开拓创新、勇于进取，扎实做好国家网络安全标准化工作。

2、中美首开高级别网络安全会议 规范网上国家行为

参考消息网 5 月 13 日消息 外媒称，根据美中两国在中国国家主席习近平去年 9 月访美时达成的共识，美国和中国于 5 月 11 日在华盛顿首次举行了旨在处理网络空间国家行为规范和其他涉及国际安全的重要问题的高级别专家组会议。据美国国务院网站 5 月 11 日报道，美中网络空间国际规则高级别专家组每年将举行两次会议。报道称，美国国务院网络事务协调员克里斯托弗·佩恩特任美方代表团团长，来自美国国务院、国防部、司法部、国土安全部等部门的代表出席了会议。中方代表团团长由中国外交部军控司司长王群担任。中方出席成员包括外交部、国防部、中央网信办、工业和信息化部、公安部等部门的代表。另据路透社 5 月 11 日报道，自从美中两国为了缓解多年来的相互指责而在去年 9 月达成反黑客协议后，高级别的美中网络安全官员 11 日举行了首次会议。报道称，美国国务院在宣布召开会议的声明中提供的有关会议的信息很少，只是说来自两国外交、国防以及其他部门的官员讨论了旨在处理网络空间国家行为规范和其他涉及国际安全的重要问题。中国外交部在简短声明中说，双方对包括国际法在内的问题进行了“积极、深入和建设性的”讨论。声明还说，中国和美

国将在未来 6 个月内适时举行下一次会议。报道称，网络安全一直是美中之间一个引发争议的问题，尽管两国保持着健康的经济关系。报道称，去年 9 月份的协议是在中国国家主席习近平访问美国期间达成的，包括两国承诺均不得为了获得商业利益而有意发动黑客袭击。

3、匿名者持续 OpIcarus 行动：又攻击了八家金融机构

网易 5 月 9 日消息 匿名者发起的 OpIcarus 行动已经有些时日，过去几天，又有八家金融机构遭到了它们的 DDoS 攻击。OpIcarus 的首个目标，是希腊中央银行，紧接着遭殃的是塞浦路斯央行。之后，受害者的数量出现了爆发式的增长，并且遍布世界各地，匿名者旗下多个团体均有涉案，比如 Ghost Squad Hackers。周末的时候，其在 Twitter 上公布了针对多米尼加央行、格恩西金融服务委员会、荷兰央行、马尔代夫央行的行动。一天之后，新闻源 HackRead 也报道了针对肯尼亚央行和 National Bank of Panama 的攻击。Ghost Squad Hackers 成员是 ege 在 Twitter 上公布了针对波西尼亚和黑塞哥维那央行的 DDoS 攻击，匿名者成员 BannedOffiline 也在 Twitter 上描述了对墨西哥央行的攻击。汇总一下，在不到一周的时间内，匿名黑客已经通过 DDoS 的手段，侵扰了名单中的 10 家金融机构（总共 160 家），美国联邦储备银行、世界银行、国际货币基金组织、纽交所、英格兰银行等大名亦在其上。

4、全球有 6 家银行遭到土耳其黑客团体攻击

网易 5 月 15 日消息 根据相关报道，土耳其黑客团体 Bozkurtlar 在上周对超过 6 家国际银行发起网络攻击并成功窃取了部分数据。在上周二，荷兰孟加拉银行（孟加拉共和国）、城市银行（孟加拉共和国）、信托银行（孟加拉共和国）、商业通用发展银行（尼泊尔）、Sanima Bank（尼泊尔）遭到攻击，随后上周四锡兰商业银行（斯里兰卡）遭到攻击。首批曝光的泄露文件容量超过 300MB，事涉 5 家银行，从这些曝光的文件中曝光数据最多的是商业通用发展银行，容量为 251MB，泄密数据涉及客户数据、手机号码、加密密码等，此外还有大部分内部银行邮件通信文件。然而这件事情远远还没有结束，在第二波曝光数据中，锡兰商业银行的泄密文件容量达到了 6.97GB，共计涵盖 158000 份文件。这些数据 Dump 包含 PHP 文件到年度银行报道，甚至还有服务器备份和银行金融声明等等。

关于国家互联网应急中心（CNCERT）

国家互联网应急中心是国家计算机网络应急技术处理协调中心的简称（英文简称为 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，是一个非政府非盈利的网络安全技术协调组织，主要任务是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展中国互联网上网络安全事件的预防、发现、预警和协调处置等工作，以维护中国公共互联网环境的安全、保障基础信息网络和网上重要信息系统的安全运行。目前，CNCERT 在我国大陆 31 个省、自治区、直辖市设有分中心。

同时，CNCERT 积极开展国际合作，是中国处理网络安全事件的对外窗口。CNCERT 是国际著名网络安全合作组织 FIRST 正式成员，也是 APCERT 的发起人之一，致力于构建跨境网络安全事件的快速响应和协调处置机制。截止 2015 年，CNCERT 与 66 个国家和地区的 165 个组织建立了“CNCERT 国际合作伙伴”关系。

联系我们

如果您对 CNCERT《网络安全信息与动态周报》有何意见或建议，欢迎与我们的编辑交流。

本期编辑：狄少嘉

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158